UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/781,311	02/18/2004	Vincent Dupaquis	ATM-244	4864

3897 7590 12/14/2007

SCHNECK & SCHNECK
P.O. BOX 2-E
SAN JOSE, CA 95109-0005

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
12/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/781,311	DUPAQUIS ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 October 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 10 October 2007 has been noted and made of record.

2. Claims 1-13 have been presented for examination.

Response to Arguments

3. Applicant's arguments, see pages 5 and 6, and amendments filed 10 October 2007, with respect to the 35 U.S.C. 112, 2nd paragraph rejections have been fully considered and are persuasive. The 35 U.S.C. 112, 2nd paragraph rejection of claims 1-13 has been withdrawn.

4. Applicant's arguments with respect to the prior art rejections filed 10 October 2007 have been fully considered but they are not persuasive.

5. The Applicant argues that Liardet does not teach randomizing of the quotient value that would be used in the modulo reduction operation itself with regards to independent claims 1 and 8 (see pages 6-7 and 8). The Examiner disagrees. As noted in the previous, and again below, Liardet teaches modifying an intermediary result with a random quantity, carrying out the calculation and restoring the expected result at the end of the modular reduction (paragraphs 0033-0035, 0041). The Applicant's claimed random quotient value is an intermediary result used in calculating the remainder R' and therefore drawn to Liardet's disclosed intermediary result that has been modified with a random quantity. As argued in the previous Office Action, It would have been obvious to one of ordinary skill in the at the time the invention was made to generate, in a random number generator, a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient $q' = q - E$, since Liardet states at paragraph 0031 that adding a random intermediary value to a calculation provides protection against attacks by differential power analysis. Therefore the rejection of independent claims 1

and 8 is maintained; subsequently, the rejection of the claims that depend from 1 and 8 are also maintained.

6. The Applicant argues that claims 2, 3, 10 and 11 use an extra word shift which has not been disclosed in Barrett's method or Liardet. The Examiner cites Sections 14.42 and 14.44 of **The Handbook of Applied Cryptography**, equation 4 on page 386 of **The Chinese Remainder Theorem and its Application in a high-speed RSA crypto Chip**, and Sections 14.42 and 14.44 of **The Handbook of Applied Cryptography** as showing at least the use of a word shit in Barrett's method. The Examiner holds that the use of an additional word shift is not novel and non-obvious. What is to prevent further applications from claiming two, three or multiple additional word shifts as their novel and non-obvious feature and getting patents? In other words, the addition of one word shift is an obvious modification unless it can be shown that the use of an additional word shift produces unexpected results, commercial success, satisfies a long-felt need in the art, or any other type of objective evidence that shows the additional word shift would not be an obvious modification. See MPEP § 2141(III). Since the Applicant has not shown that the use of an additional word shift would not be an obvious modification, the rejection of claims 2, 3, 10, and 11 has been maintained.

7. Applicant's arguments, see page 9, filed 10 October 2007, with respect to the double patenting rejection have been fully considered and are persuasive. The double patenting rejection of claims 1-13 has been withdrawn.

8. See further rejections set forth below.

Terminal Disclaimer

9. The terminal disclaimer filed on 10 October 2007 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of Application No. 11/203,939 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Claim Rejections - 35 USC § 103

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barrett's modular reduction method in view of U.S. Patent Application No. 2003/0044014 A1 to Liardet et al., hereinafter Liardet.

12. As per claim 1, Barrett's method involves precomputing and storing in memory a constant U representing a bit-scaled reciprocal of a modulus M and estimating an approximate quotient q for a number X to be reduced modulo M, wherein said estimating is executed upon X in a computation unit by a multiplication by said constant U and by bit shifts of X and a shift of said multiplication as shown by page 5, lines 8-13 of Applicant's specification. This is further supported by pages 603-605 of **The Handbook of Applied Cryptography**, which was submitted in the IDS of 27 April 2005. Barrett's method also calculating a remainder R' = X - q'M in said computation unit, said remainder being larger than said modulus M but congruent to X modulo M, as shown by Equation 1, of Section 2.2 on page 385 of **The Chinese Remainder Theorem and its Application in a high-speed RSA crypto Chip**, which was submitted by the Applicant in the IDS of 27 August 2004.

13. Barrett's method does not disclose generating in a random number generator a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient $q' = q - E$.

14. Liardet teaches modifying an intermediary result with a random quantity, carrying out the calculation and restoring the expected result at the end of the modular reduction (paragraphs 0033-0035, 0041).

15. It would have been obvious to one of ordinary skill in the at the time the invention was made to generate, in a random number generator, a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient $q' = q - E$, since Liardet states at paragraph 0031 that adding a random intermediary value to a calculation provides protection against attacks by differential power analysis.

16. Regarding claims 2 and 10, Barrett's method teaches wherein precomputing said constant U is performed according to the equation $U = [b^{2n+1}/M]$, where $b = 2^w$, with w being the word size of the computation unit in bits, as show via evidentiary evidence of Sections 14.42 and 14.44 of **The Handbook of Applied Cryptography**. This is further supported equation 4 on page 386 of **The Chinese Remainder Theorem and its Application in a high-speed RSA crypto Chip**.

17. With regards to claims 3 and 11, Barrett's method teaches wherein computing the estimated quotient q is performed by the computation unit according to the equation $q = [([X/b^n]$

$\cdot U) /b^{n+2}]$, as show by evidentiary evidence of Sections 14.42 and 14.44 of **The Handbook of Applied Cryptography**.

18. Concerning claims 4 and 12, Barrett's method teaches wherein a supplemental subtraction by one is included in the computing of the estimated quotient value, as show via evidentiary evidence of Section 2.2 of **The Chinese Remainder Theorem and its Application in a high-speed RSA crypto Chip**.

19. Regarding claim 5, Liardet teaches wherein the modular reduction of X is part of a computer hardware-implemented cryptography program (paragraphs 0002, 0041).

20. Regarding claim 6, Liardet does not teach wherein an alternate calculation pathway is provided wherein generating and applying an error value to the approximate quotient may be selectively omitted. The Examiner notes that if the applying the error value to the approximate quotient is omitted, claim 1 recites Barrett's method.

21. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a selection process for including the error value, since it would have only required routine skill in the art to include the alternate path of omitting the error value. See MPEP § 2144.04; see *In re Kuhle*, 526, F.2d 553, 188 USPQ 7 (CCPA 1975).

22. Regarding claims 7 and 13, Barrett's method teaches wherein the random number generator has a specified error limit of one-half word, whereby $0 <= E < (2^{w/2} - 1)$, as show by evidentiary evidence of Section 14.43 of **The Handbook of Applied Cryptography**.

23. Claims 8-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admitted Prior Art in view of Barrett's Method, and further in view of Liardet.

24. As per claim 8, Applicant's admitted prior art discloses computational hardware for executing a cryptographically secure modular reduction method, the hardware comprising a computation unit adapted to perform word-wide multiply and accumulate steps on operands retrieved from a memory and carry terms from a set of registers and an operations sequencer comprising logic circuitry for controlling the computation unit as discussed from page 3, line 23 to page 4, line 9. Barrett's method, as disclosed by page 5, lines 8-13 of Applicant's specification is a method to carry out a modular reduction of a number X with respect to a modulus M that involves at least an estimation of an approximate quotient q from a pre-stored constant U representing a bit-scaled reciprocal of the modulus and calculation of a remainder value $R' = X - q'M$.

25. As established by the Applicant the prior art does not show the above systems with a random number generator for generating a random error value E; and calculating a randomization of said the approximate quotient with said random error value E to obtain a randomized quotient $q' = q - E$.

26. Liardet teaches modifying an intermediary result with a random quantity, carrying out the calculation and restoring the expected result at the end of the modular reduction (paragraphs 0033-0035, 0041).

27. It would have been obvious to one of ordinary skill in the at the time the invention was made to generate, in a random number generator, a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient $q' = q - E$, since Liardet states at paragraph 0031 that adding a random intermediary value to a calculation provides protection against attacks by differential power analysis.

28. Regarding claim 9, Applicant's admitted prior art teaches operation parameter registers accessible by said operations sequencer, said registers containing any one or more of (a) pointers for locating operands within said memory, (b) information about lengths of operands, (c) carry injection control information for carry term registers, and (d) destination address information for intermediate results of operation steps (page 3, line 35 to page 4, line 2).

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

30. The following patents are cited to further show the state of the art with respect to adding random information to cryptographic calculations, such as:

United States Patent No. 7,073,072 B1 to Salle, which is cited to show thwarting power dissipation attacks by adding random information to cryptographic calculations.

31. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

32. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

33. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

34. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

35. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf